REMARKS

Priority Claim

Applicants request that the Office respond to the claim to priority made in the preliminary amendment received by the Office on Dec. 22, 2004.

Status of Pending Claims

Claims 1-66 are pending after entry of the foregoing amendment. Claims 1-64 stand rejected. Claims 65 and 66 are new. Support for the new claims can be found at least at page 8, ll. 1-10 of the Present Application. No new matter has been added by this amendment.

Claims 1-24 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Benson et al. (U.S. patent 7,051,199) ("Benson"). Claims 25-64 stand rejected under 35 U.S.C. § 103(b) as being obvious over Benson.

Claims 1 -- 64 are Patentable Over the Cited Prior Art

Claim 1, recites in part:

> operable to provide cryptographic services requested by said at least one remote device via said secure network interface engine,
> wherein said cryptographic service requests are comprised of input data to be transformed;
> **at least one unique identifier for identifying at least one key for performing the transformation**; and
> instructions for how the cryptographic service engine should transform the data

The bolded elements are not disclosed or suggested by the cited prior art. In Benson, the actual first key and optionally the actual second key are sent to the server. Benson, *c.* 10, *ll.* 40 -- 57. In contrast, the bolded elements recited above send a "unique identifier for identifying at least one key for performing the transformation." In Benson, there is no teaching or suggestion of sending a unique identifier to the key that performs the encryption services. The bolded elements provide at least the advantage of being able to provide centralized storage and management of the keys. Additionally, in Benson, the first key is for

encrypting messages to and from the server and not for performing encryption services on the server.

Therefore, withdrawal of the rejection of claim 1 is requested. Additionally, since claims 2-25 depend directly or indirectly from claim 1, withdrawal of the rejections of claims 2-25 is requested for at least the same reasons as for claim 1. Additionally, since claims 26-64 were rejected for reciting the same or similar limitation as claims 1-25, withdrawal of the rejections of claims 26-64 is requested for at least the same reasons as for claims 1-25.

Claim 9 Recites Additional Patentably Distinct Elements

Claim 9, recites in part:

> wherein said encryption and decryption functions comprise:
> DES, 3DES, AES, RSA, DSA, ECC, RC6, MARS, Twofish, Serpent, CAST-256, DESX, RC2, RC5, Blowfish, Diamond2, TEA, SAFER, 3-WAY, Gost, SHARK, CAST-128, Square, Shipjack, ECB, CBC, CTS, CFB, OFB, counter mode(CTR), Panama, ARC4, SEAL, WAKE, Wake-OFB, Blumblumshub, ElGamal, Nyberg-Rueppel (NR), Rabin, Rabin-Williams (RW), LUC, LUCELG, DLIES (variants of DHAES), ESIGN padding schemes for public-key systems: PKCS#1 v2.0, OAEP, PSSR, IEE P1363 EMSA2, Diffie-Hellman (DH), Unified Diffie-Hellman (DH2), Menezes-Qu-Vanstone (MQV), LUCDIF, XTR-DH, ECDSA, ECNR, ECIES, ECDH, ECMQV, SHA1, MD2, MD4, MD5, HAVAL, RIPEMD-160, Tiger, SHA-2 (SHA-256, SHA-384, and SHA-512), Panama, MD5-MAC, HMAC, XOR-MAC, CBC-MAC, DMAC, Luby-Rackoff, MDC, ANSI X9.17 appendix C, PGP's RandPool, PBKDF1 and PBKDF2 from PKCS #5

Benson does not disclose or suggest these encryption and decryption functions. Additionally, Benson does not disclose any symmetric algorithm for the "second key", which is used in Benson for the encryption services.

For at least these additional reasons, withdrawal of the rejection of claim 9 is requested.

Claims 12 and 13 Recite Additional Patentably Distinct Elements

Claim 12, recites in part: "said cryptographic service engine is operable to perform **hashing operations".** The bolded elements are not disclosed or suggested by Benson. The cited portions of Benson simply do not disclose hashing operations. See Benson, c. 5, ll. 44-67, c. 6, ll. 44-67.

Claim 13, recites in part: "wherein said **hashing operations includes HMAC with SHA-1**". The bolded elements are not disclosed or suggested by Benson. The cited portions of Benson simply do not disclose hashing operations. See Benson, c. 5, ll. 44-67, c. 6, ll. 44-67.

For at least these additionally reasons, withdrawal of the rejections to claims 12 and 13 is requested.

Claim 19 Recites Additional Patentably Distinct Elements

Claim 19 recites in part: "a private key engine, said private key engine operable to provide private keys for use by said cryptographic service engine in performing cryptographic services." Benson does not disclose or suggest the elements of claim 19. The cited portion of Benson refers to the first key which is used for creating the tunnel and not the second key which is used for the cryptographic services.

For at least these additional reasons, withdrawal of the rejection to claim 19 is requested.

Claim 23 Recites Additional Patentably Distinct Elements

Claim 23 recites in part: "wherein said private keys are loaded into said hardware security module and stored in an encrypted format." Benson does not disclose or suggest the elements of claim 23. The cited portion of Benson does not refer to storage of the second key at the cryptographic server, but rather refers to the first key which is the key used for establishing the tunnel.

For at least these additional reasons, withdrawal of the rejection to claim 23 is requested.

Claim 24 Recites Additional Patentably Distinct Elements

Claim 24 recites in part: "wherein said private keys are loaded into said hardware security module via a smart card storing said encrypted private keys.." Benson does not disclose or suggest the elements of claim 23. The cited portion of Benson does not refer to smart cards nor to using smart cards to load the second keys into memory at the server.

For at least these additional reasons, withdrawal of the rejection to claim 24 is requested.

Claim 65 Recites Additional Patentably Distinct Elements

Claim 65, recites in part:

wherein said at least **one key is generated and stored on said cryptographic key server without being transmitted across said network**

The bolded elements are not disclosed or suggested by Benson. Benson does not teach or suggest the key being generated and stored on cryptographic server without being transmitted across the network.

The bolded elements provide at least the advantage of providing centralized storage and management of the keys.

For at least these additional reasons, claim 65 is allowable.

Claim 66 Recites Additional Patentably Distinct Elements

Claim 66, recites in part:

wherein said at least one **key is a symmetric key** generated and stored on said cryptographic key **server** without being transmitted across said network.

The bolded elements are not disclosed or suggested by Benson. In Benson, the first key may be a symmetric key, but there is no teaching or suggestion in Benson of the key that is used to perform cryptographic services being a symmetric key.

The bolded elements provide at least the advantage of being able to provide both symmetric and asymmetric encryption services.

For at least these additional reasons, claim 66 is allowable.

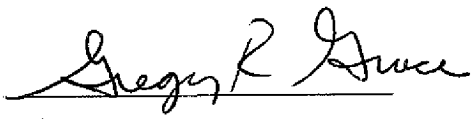
Conclusion

In view of the foregoing remarks, Applicants respectfully submit that all pending claims are in condition for allowance and a notice of allowance is respectfully requested.

The Examiner is invited to contact the undersigned by telephone at the Examiner's discretion.

Respectfully submitted,

THOMAS FOUNTAIN, ET AL.

BY: 

GREGORY R. GRACE
Registration No. 59,733
Tel: (215) 9880-2940
Fax: (215) 988-2757
Attorney for Applicants

January 4, 2009